SEPTEMBER 2024

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

BRIEF

ARTIFICIAL INTELLIGENCE IN DEFENCE OF UKRAINE

RUSSIA'S WAR IN UKRAINE SERIES 2
NO. 6

VITALIY GONCHARUK

Russia's full-scale war in Ukraine is the first international conflict in which the opposing sides have actively developed and used artificial intelligence (AI) for military purposes. AI solutions for geospatial intelligence, operations with unmanned systems, military training, and cyber warfare have been key to success on the battlefield. This brief explores the state of defence AI in Ukraine and highlights the main lessons that can be learned from the Ukrainian experience.

In 2019, Ukraine set up the Ministry of Digital Transformation to promote automation and digitisation in the public sector and in 2020 established within it the Expert Committee on the Development of Artificial Intelligence.[1] In 2021, it released a strategy for integrating AI into its military-industrial complex.[2] International companies such as Amazon, Lyft, Google, Samsung, and Grammarly have recognised Ukraine as a leading country for AI research and development (R&D) and established local R&D offices. However, Ukraine's reputation for bureaucratic inefficiency, corruption, and political interference has discouraged IT leaders from collaborating with the state-owned firms that dominate the defence sector.[3]

Ukraine has been at war for over ten years. Its strong civil society, and the use of military drones and AI are not recent developments. For example, volunteer organisations have long used AI to combat sustained information warfare by debunking fake media, exposing bot networks, and pushing back against narratives that target Ukraine's reputation.[4] They have, since 2014-15, developed valuable tools such as Kropyva, a situational awareness system, and the GIS Arta app, dubbed 'artillery Uber,' that speed up and help synchronise artillery targeting and are deployed at scale today to great effect.[5]

Since their beginnings in 2014, these non-profit and volunteer organisations have become increasingly decentralised. This has yielded certain advantages, particularly in attracting and retaining skilled drone engineers and AI innovators. Early distribution networks could also benefit from candid, well-established feedback loops from the front. The Ukrainian government recognised the expertise of these groups and sought their cooperation. When the full-scale invasion began, private enterprises and volunteer organisations stepped up to pioneer the use of first-person-view (FPV) drones and bring the first AI-assisted equipment to the trenches and command posts, often relying on personal networks with soldiers or units. After the initial shock of the invasion and the successful counteroffensives of spring and autumn 2022, the government focused again on stimulating AI innovation in the defence sector.[6]

When the full-scale invasion began, private enterprises and volunteer organisations stepped up to pioneer the use of first-person-view (FPV) drones and bring the first AI-assisted equipment to the trenches and command posts

New Defence AI Priorities

In 2023, the Expert Committee released revised priorities for the development of AI.[7] They include AI for domestically produced uninhabited systems to allow for autonomous navigation (without relying on GPS), task selection, information gathering, and weapons detection and identification. A strategic partnership between the Ukrainian government and private foundations aims to provide Ukraine with a battlefield advantage in this area.[8]

A second priority is AI that can identify and flag disinformation and the bot networks that spread it. This includes tools to quickly detect deepfake audio and video clips made with the assistance of generative AI. Other countries can also share datasets, using AI to cooperate more effectively against foreign information influence campaigns.

In logistics, another priority, predictive AI can help schedule maintenance, pre-empt shortages at military warehouses, and anticipate potential obstacles to the resupply of missions by simulating the operational environment in advance. Meanwhile, uninhabited logistics vehicles with AI navigation systems can deliver supplies and evacuate casualties.[9]

AI-powered solutions are no longer optional for Ukraine but are crucial for safeguarding lives and national security

AI is also an important tool for consolidating data gathered from various sources (satellites, drones, robots, etc.) for mine and ammunition detection and neutralisation. A better understanding of minefield locations and density allows more effective neutralisation plans to be developed, while using robots equipped with AI to clear mines and unexploded ordnance makes the task safer.

A further priority is AI for cybersecurity and defence sector information and communications technology. Here, AI can support tapping into enemy communications networks and enhancing electronic warfare (EW) operations. It can also strengthen data encryption and exchange networks, while AI-powered cybersecurity systems can automatically identify, analyse, and classify threats, enabling swifter and more effective responses.

A final priority is the creation of conditions that can facilitate the rapid development of AI solutions for security and defence. This includes legislation to address transparency, standardisation efforts, and streamlined protocols for licensing and imports.

This wide range of AI applications is particularly important in enhancing awareness, readiness, and capabilities during wartime, including through simulating combat training scenarios, monitoring surveillance video, scraping and analysing open-source data, facial recognition analysis, reconnaissance, and damage assessment. It also boosts the domestic manufacture of dual-use products, such as thermal cameras, sensors, and drones.

Russia's own significant AI investments, meanwhile, also require swift responses. AI-powered solutions are no longer optional for Ukraine but are crucial for safeguarding Ukrainian lives and national security, even if creating specific solutions for the battlefield requires significant resources. To remain competitive in defence AI over the coming 2–3 years, Ukraine must match Russia's investments. The Expert Committee has thus also recommended specific grants and dedicated structures to ensure effective project implementation for projects with a greater than 6-month timeframe.

Defence AI Ecosystem

Although a decentralised defence sector has brought certain benefits to Ukraine, it has also led to coordination and standardisation problems, which are being addressed.[10] The government fosters collaboration, synchronisation, and knowledge exchange within the AI community, with the aim of creating a more efficient ecosystem that unites the efforts of state entities, private foundations, volunteer organisations, and foreign companies in satisfying defence requirements.[11]

Reaching this goal is complicated by several key obstacles that need to be addressed. These include corruption and conflicts of interest. Transparency and ethical conduct within the

government and stakeholder groups are crucial for fostering trust and efficient resource allocation. Defeating attempts by Russia and other actors to disrupt or manipulate the development and deployment of AI-powered defence solutions is also paramount.

A shortage of essential skilled personnel, meanwhile, requires initiatives to attract, train, and retain managers and AI engineers with expertise in military applications. And more efforts are needed to encourage open collaboration and knowledge-sharing among all stakeholders, including foreign companies.

Even so, the war has become a crucible for commercial innovation.[12] Ukrainian companies have developed a variety of AI solutions that are used on the battlefield and in other defence and security applications, for example: uninhabited aerial and ground vehicles for a wide range of tasks including reconnaissance, surveillance, fire adjustment and support, target identification and engagement, logistics, and evacuation; electronic warfare systems to help shield cities from enemy drones; neural networks of acoustic sensors; and training and simulation systems.

Ukraine has also become a testbed where foreign companies can deploy and improve their AI-enabled products. These include data fusion and decision assistance tools, terminal guidance software for FPV drones, and facial recognition software to identify enemy combatants and collaborators.[13]

These AI solutions deliver at least three advantages: they free up personnel for core duties by automating complex tasks like data analysis; they enhance and speed up decision-making through high-precision analysis, thus blunting some of Russia's advantages; and, most importantly, they save lives in hazardous reconnaissance and mine clearance operations.

Governance Issues

Throughout the war, the Ukrainian government has accumulated a substantial amount of information about citizens, raising concerns about compliance with privacy laws and questions about whether such legal provisions should remain active under martial law. Furthermore, the question of data retention and usage after the war remains unanswered. A robust legal framework for data governance is needed to address these issues as fostering a transparent approach to data governance will ensure that Ukraine's AI advancements remain a force for good while also safeguarding citizen privacy. EU integration necessitates aligning Ukraine's data privacy laws with European standards and will eventually strengthen data protection and build trust.

These EU requirements and emerging global norms for responsible and safe AI, however, do not always consider the circumstances under which democratic countries operate in wartime. Ukraine has, nonetheless, taken steps to demonstrate a commitment to responsible AI governance, even amidst the ongoing war. For example, representatives of the Expert Committee and relevant ministries are actively involved in the development of new policy frameworks, including the Bletchley Declaration and the Political Declaration on Responsible Military Use of AI and Autonomy.

AI solutions free up personnel for core duties, enhance and speed up decision-making, save lives in hazardous operations

Conclusion

After two years of intense fighting, Ukraine and Russia are competing to improve existing defence solutions with AI and to develop new AI-powered systems. The war has forced Ukraine to focus on what works best on the battlefield to blunt the enemy's advantages while also considering future warfighting needs. This has led to a clear focus on providing the best solutions for frontline troops and developing a talent pipeline for technology development.

The advances in defence AI in this war will shape future international discussions on its use in warfare. NATO countries should monitor these developments to understand the impact on their own military planning and R&D priorities. Violent non-state actors will also likely learn from this conflict and try to use AI themselves. Efforts to

prevent AI technology from falling into their hands will be needed.

Countries will also need to update their data and privacy protection policies, which are not suitable for wartime. In war, collecting, analysing, and sharing large amounts of public and private data can provide major advantages in areas such as intelligence, strategic communication, civil defence, or mobilisation. A realistic view on the legal restriction of human rights in wartime is needed and a redefinition of the 'human in the loop' principle will be crucial for future certification standards and AI compliance and verification.

Finally, crowdsourcing, open-source technology, decentralisation, and volunteer efforts have been vital in Ukraine's defence and should be studied to see how they can drive defence innovation elsewhere.

Endnotes

[1] Cabinet of Ministers of Ukraine, *Кабінет Міністрів України Розпорядження від 2 грудня 2020 р. № 1556-р Київ Про схвалення Концепції розвитку штучного інтелекту в Україні* [On the approval of the Concept for the development of artificial intelligence in Ukraine. Order of the Cabinet of Ministers of Ukraine No.1556-p], (Cabinet of Ministers, December 2020).
[2] President of Ukraine, *Указ Президента України №121/2021 Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України»* [On the Strategy of military security of Ukraine" Decree of the President of Ukraine No. 121/2021] (President of Ukraine, March 2021).
[3] Kateryna Bondar, "Arsenal of Democracy: Integrating Ukraine Into the West's Defense Industrial," Carnegie, 4 December 2023.
[4] Inna Volosevyvh, "Ukraine: Results of the Revolution of Dignity. How have the country and the people changed," *Vox Ukraine*, 31 August 2016.
[5] Stephen Bryen, "Musk's tech put to deadly weapon effect in Ukraine," *Asia Times*, 1 July 2022; Tom Cooper, "Kropyva: Ukrainian Artillery Application," *Medium*, 10 June 2022.
[6] Ministry of Digital Transformation of Ukraine, "Ukraine launches BRAVE1 defence tech cluster to stimulate development of military innovations and defence technologies," Government Portal, 26 April 2023.
[7] Expert Committee on AI, *Regarding critical development priorities of artificial intelligence technologies in the field of security and defense of Ukraine [unofficial translation],* trans. Vitaliy Goncharuk (Kyiv: Ministry of Digital Transformation of Ukraine, August 2023).
[8] Joe Saballa, "Ukraine's 'Army of Drones' Destroys 200 Russian Targets in One Week: Minister," *The Defense Post*, 14 September 2023.
[9] Oleksander Shumilin, "Ukraine to massively produce robotic ground platforms that can fire, lay mines or evacuate people – photo," *Ukrainska Pravda*, 12 March 2024.
[10] The Verkhovna Rada of Ukraine, "Мінстратегпром задумувався як потужний центр координації промислової політики та військово-промислового комплексу - Дмитро Кисилевський [Minstrategprom was conceived as a powerful center for coordinating industrial policy and the military-industrial complex – Dmytro Kysilevsky]," Press Service of the Office of the Verkhovna Rada of Ukraine, 23 March 2023.
[11] Jenna McLaughlin, "How Ukraine's tech experts joined forces with the government despite differences," *NPR,* 6 December 2023.
[12] Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab," *Time*, 8 February 2024, Robin Fontes and Jorrit Kamminga, "Ukraine A Living Lab for AI Warfare," *National Defence*, 24 March 2024.
[13] Vera Bergengruen, "How Tech Giants"; David Hambling, "Destroying Russian Tanks Is Just The Start For U.S. AI Drone Autopilot," *Forbes,* 10 July 2024; Vera Bergengruen, "Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company," *Time*, 14 November 2023.

About the author

Vitaliy Goncharuk
Vitalii Goncharuk is a member of the AI Committee of Ukraine and the founder of TechWise Society Foundation in Washington, DC, USA

ICDS.Tallinn
@ICDS_Tallinn
ICDS-Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076